Electronic Version
Stylesheet Version v1.1.1

# Claims

[c1] A method for recognizing parties with whom a user or system has established a trusted relationship by utilizing a computerized database to match public keys. The database will record contain information about trusted relationships, which may include but is not limited to, public key of a trusted party, public and private key of this user or system in the trusted relationship, domain name of a trusted party, and other information that may be pertinent to a trusted relationship.

[c2] A method for creating, storing and extracting embedded text, electronic signatures, and public keys and/or certificates encoded into a graphical image, including but not limited to any and all of the following, a digital certificate or public key, the electronic signature of a document, the electronic signature of the graphical image, and any additional information deemed necessary by the party or agent creating the image.

[c3] A method utilizing the graphical image defined in claim 2 for extracting the public key or certificate stored in the graphical image and for detecting whether the key belongs to a trusted party in the trusted party database as

defined in claim 1.

[c4] A method for using drag-and-drop user action to extract the public key or certificate stored in the graphical as defined in claim 3 comprising of the steps: (a) drag-and-drop a document or graphical image to the Trusted Keys database; (b) verifying the signatures in the graphic image; (c) extracting the public key or certificate to determine if it belongs to a trusted party in the database; and (d) at the user's option, establishing a secure connection using any standard protocol that accepts certificates or public/private keys and does not require account names and passwords to authenticate the user or server.